CLAIMS

1. A circuit design method executed by a computer for designing a processing circuit for processing on a finite field comprising:

a first step of obtaining a first primitive root α_1 on the basis of a first polynomial for a first extension from a first finite field to a second finite field;

a second step of obtaining a second primitive root α_2 on the basis of a second polynomial for a second extension from said second finite field to a third finite field, in which a coefficient of a 0-th term is defined using said first primitive root α_1 obtained in said first step and the coefficient of the 0-th term of said first polynomial;

a third step of defining the processing on said third finite field using a base expressed using said second primitive root α_2 obtained in said second step; and

a fourth step of designing a processing circuit for the related processing on the basis of the processing defined in said third step.

2. A circuit design method as set forth in claim 1, wherein when:

said first finite field is an extension of an

extension order n from a finite set F_q,

said second finite field is a first extension of an extension order l_1 from said first finite field,

said third finite field is a second extension of an extension order l_2 from said second finite field, and

defining the processing on said third finite field shown by the following (1-2) of the order shown by the following (1-1) in the third step, the method

obtains said first primitive root α_1 on the basis of the following (1-3) in the first step and

obtains said second primitive root α_2 on the basis of the following (1-4) in the second step:

$$q^{n \cdot \ell_1 \cdot \ell_2} \quad (q=p^m,\ p\text{: prime number},\ n,\ l_1,\ l_2,\ m\text{: natural numbers}) \qquad (1\text{-}1)$$

$$L := F_{q^{n \cdot \ell_1 \cdot \ell_2}} \qquad (1\text{-}2)$$

$$\alpha_1 : \alpha_1^{l_1} - \alpha_1 + c = 0, \quad X^{l_1} - X + c \in F[X],\ \mathit{Irreducible} \qquad (1\text{-}3)$$

$$\alpha_2 : \alpha_2^{l_2} - \alpha_2 + a = 0, \quad a = c^{-1} \cdot \alpha_1^{i} \cdot \exists i \in Z,$$
$$s.t.\ X^{l_2} - X + a \in K[X],\ \mathit{Irreducible} \qquad (1\text{-}4)$$

3. A circuit design method as set forth in claim 2, wherein,

when said extension orders l_1 and l_2 are both q, the method

obtains said first primitive root α_1 on the basis of the following (1-5), (1-5a) in the first step and

obtains said second primitive root α_2 on the basis of the following (1-6) in the second step:

$$\alpha_1 : \alpha_1^q - \alpha_1 + c = 0, \qquad \exists c \in F s.t. Tr_{F_q}^{F}(c) \neq 0$$

(1-5)

$$Tr_{F_q}^{F}(c) := c + c^q + c^{q^2} \qquad c^{q^3} + \cdots + c^{q^{n-1}}$$

(1-5a)

$$\alpha_2 : \alpha_2^q - \alpha_2 + a = 0, \qquad \exists a = c^{-1} \cdot \alpha_1^i \in K,$$

$$i \in Z s.t. Tr_{F_q}^{K}(\alpha_1^i) \neq 0;$$

(1-6)

4. A circuit design method as set forth in claim 1, further comprising:

defining processing on said third finite field using processing on said second finite field in said third step and

designing a first processing circuit for processing on said second finite field used in said third step and designing a second processing circuit for processing on said third finite field using said first

processing circuit.

5. A circuit design method as set forth in claim 4, further comprising defining processing on said third finite field using processing on said second finite field multiplying a coefficient of the 0-th term of said second polynomial in said third step.

6. A circuit design apparatus for designing a processing circuit for processing on a finite field comprising:

a first means for obtaining a first primitive root α_1 on the basis of a first polynomial for a first extension from a first finite field to a second finite field;

a second means for obtaining a second primitive root α_2 on the basis of a second polynomial for a second extension from said second finite field to a third finite field, in which a coefficient of a 0-th term is defined using said first primitive root α_1 obtained by said first means and the coefficient of the 0-th term of said first polynomial;

a third means for defining processing on said third finite field using a base expressed using said second primitive root α_2 obtained by said second means; and

a fourth means for designing a processing

circuit for the related processing on the basis of the processing defined by said third means.

7. A program executed by the circuit design apparatus for designing a processing circuit for processing on a finite field comprising:

a first routine of obtaining a first primitive root α_1 on the basis of a first polynomial for a first extension from a first finite field to a second finite field;

a second routine of obtaining a second primitive root α_2 on the basis of a second polynomial for a second extension from said second finite field to a third finite field, in which a coefficient of a 0-th term is defined using said first primitive root α_1 obtained in said first routine and the coefficient of the 0-th term of said first polynomial;

a third routine of defining processing on said third finite field using a base expressed using said second primitive root α_2 obtained in said second routine; and

a fourth routine of designing a processing circuit for the related processing on the basis of the processing defined in said third routine.